

To all whom it may concern:

Colin Hendrick

SYSTEM FOR AUTOMATIC CONNECTION TO A NETWORK

of which the following is a full, clear and exact description.

SYSTEM FOR AUTOMATIC CONNECTION TO A NETWORK

Ins A17

TECHNICAL FIELD

The present invention relates to a computer system that allows a user to automatically connect to a network service provider, and more particularly, to a system and method which allows a user to automatically connect to a network service provider by using a data card (i.e., a "smart card"). A smart card is a card that is approximately the size of a credit card and stores electronic data on a microchip for use in a variety of applications. The present invention also relates to an online advertisement system that accesses user profile information stored on a smart card to provide advertisements specifically tailored to the user's profile. The present invention also relates to a system for managing digital rights of digital content over a network.

BACKGROUND ART

With the increasing use of information technology to access and exchange information over a network, in addition to the emergence of commercial transactions which have been taking place over open networks such as the internet, it has become necessary to store information (particularly about a user) in a secure manner. One method of securing information is by a smart card. A smart card is approximately the size of a conventional credit card; however, instead of having a magnetic strip which stores data on the card, smart cards usually have a microchip embedded within their structure. The microchip stores information in the form of electronic data which may be of use to the smart card user.

Essentially, smart cards can be categorized into two distinct types, namely "contact smart cards" and "contactless smart cards." Smart card readers are devices that read information contained in a smart card microchip. They are typically

connected to a computer so that information in the smart card chip can be relayed to the computer.

5 "Contact" smart cards are typically inserted into a smart card reader. These cards have a microchip on one side of the card which makes contact with an electrical connector contained within the smart card reader. Data is exchanged between the chip on the smart card and the electrical connector of the smart card reader.

10 "Contactless" smart cards do not have an exposed chip on one side of the card, but have an antenna embedded within the card itself. The antenna transmits information to a coupler unit or "smart card reader" which is also fitted with an antenna. The antenna allows information to be exchanged without physical
15 contact having to be made between the smart card chip and the smart card reader.

Typically when a smart card is inserted into a reader mechanism, the embedded chip transmits a message to the host machine on which the reader is attached. This message
20 typically acknowledges card insertion into the reader mechanism.

Existing applications that utilize the smart card are launched by a human user after the smart card is inserted or before the
25 smart card is inserted. In the general case of application launch before card insertion a prompt within a typical application requires users to insert and then acknowledge card insertion through a prompt. In the general case of application launch after card insertion a similar acknowledgment is also
30 required.

Internet Service Providers (ISPs) or Internet Access Providers (IAPs) are companies that provide individuals and companies

with access to the internet and to other related services, such as website building and hosting. A user of an internet service typically accesses the ISP from his or her computer via a telephone line so as to gain access to the internet. The ISP usually requires the user to enter particular information in relation to the user, such as a login name and password which is then checked against the ISP's database to verify that the user is registered with the ISP. Traditionally ISPs have been located within their own regional areas and therefore the user typically dials a local number to access the ISP.

Problems can occur when the user uses his or her computer to log on to the ISP (e.g., such as on a business trip using a laptop computer) and the number recorded in the computer for the ISP may be different (i.e., different area and/or country code). It is then necessary for the user to enter in the area code (or country number if he or she is overseas) for the ISP and pay for a long distance call. Alternatively, the same ISP may have a local number within the particular locale in which the user is located at a particular time. However, the user typically has to physically search for the local ISP number in the particular locale in which he or she is located. Furthermore, delays in the time it takes for a user to access the internet can result whenever the user is in a different geographic location or happens to use a different computer.

Moreover, there is a need for a simple way to provide advertisements to a user which are specifically directed to that user's tastes and characteristics.

Another issue arising from the increasing use of information technology to access and exchange information over a network is digital rights management. Consumer demand in the market for online books, magazines, music, software and games is dramatically increasing. The increased demand makes it even

more important that creators and publishers be assured that their rights will be safeguarded, their content protected, their payments collected, and their profits maintained. At the same time, consumer demand for easier access to content, greater convenience, and lower prices must be met.

Some of the specific areas involved in digital rights management include the purchase and download of e-books and software. Also included is the pay per view or download of valuable and timely printed material (such as industry newsletters), digital video, and digital music.

There is a need for a more effective and more efficient system for controlling access to and usage of various forms of digital data, while ensuring that the necessary information is secure.

DISCLOSURE OF INVENTION

The present invention is directed to overcoming the problems in the prior art regarding the inconvenience of the user having to physically search for the local ISP number in the particular locale in which he or she is located, or the increased cost in paying for a long distance call if this search is not performed, or the delays in time it takes for a user to access the internet when the user is in a different geographic location or happens to use a different computer.

The present invention is also directed to an online advertisement system that accesses user profile information stored on a smart card to provide advertisements specifically tailored to the user's profile.

The present invention is also directed to a system and method for managing digital rights of digital content over a network.

According to one embodiment of the present invention, there is disclosed a computer system for allowing a user to automatically access one of a plurality of network service providers which require information specific to the user and/or the network service provider to be accessed, the computer system comprising:

a data card which contains the information specific to either the user and/or the network service provider to be accessed;

a data card reader adapted to access at least part of the information contained on the data card when the data card is in communication therewith;

a data processor in communication with the data card reader and adapted to be connected to a network;

an application program resident on the data processor, the application program being configured to automatically retrieve at least part of the information contained on the data card when the data card is in communication with said data card reader and to use the information to gain access to one of the plurality of network service providers via the network by using one of a default access number indicating a designated network service provider and a local access number from a database containing a list of access numbers for the plurality of network service providers along with corresponding location information for each access number in the list,

wherein the application program is immediately triggered upon insertion of the data card into the data card reader.

The data card typically comprises a microprocessor for processing the information stored within the data card, a memory component which enables the information to be stored

within the data card and a communications interface for transferring the information from the data card to the data card reader.

5 The communications interface may include an antenna embedded inside the data card so as to communicate the information between the data card and the data card reader. In such an embodiment, the data card reader also has an antenna embedded inside so as to receive/relay information from/to the data
10 card.

Alternatively, the communications interface may include a contact connector and the data card reader may include electrical connectors so that information can be
15 received/relayed from/to the data card when the contact and the electrical connectors are in physical contact. The communications interface of the data card may make contact with a communications interface located on the data card reader. In some embodiments of the invention, the data card is a smart card and the data card reader is a smart card reader. The data
20 card may also contain a battery for storage of power received from the data card reader when it is connected thereto.

Preferably, the data card is inserted into a recess provided
25 within the data card reader. Typically, when the data card is inside the data card reader, the electrical connectors on the data card reader detect that a data card is inserted in the data card reader and an activation code is generated by the microprocessor and is sent to the data processor. The
30 activation code is then sent to the application program.

When the activation code is received by the data processor, the application program instructs the CPU to generate a code to establish a link with the network service provider by
35 instructing a modem to dial a default number to access the

network service provider via the network. Hence, by inserting the smart card into the smart card reader, a connection is automatically established with the network service provider. The default number may be the number of a network service provider local to the user. If the dial-up sequence is via a network such as a telephone line, the phone number of the network service provider may be part of the specific information contained on the data card.

If the user is located in another city or indeed in another country, there will be a different country and area code required and the number dialed by the application program will not connect to the network service provider. In such a situation, the application program will also include a logic code which determines that a connection has not been made and shall generate a message to the user requesting that they input the country and/or the city in which they are currently located.

Optionally, the application program may contain a database detailing a list of the countries, the associated locale by area codes within those countries and may also include a list of network service providers within each country and local area location. In some embodiments of the invention, the message generated by the application program may generate from the database, the list of countries on a graphical display. Typically the user will then select the country he or she is located in at a particular time. Once the country is selected, the application may then generate from the database, a list of locales by area code associated with the selected country. The user then selects the locale in which he or she is located. The application program then notes the locale and retrieves from the database, the country code and/or the area code of the location.

Alternatively, the database may be stored on a memory means such as a compact disc read only memory (CD ROM) accessible by the data processor. Or, the database may be stored in a remote server accessible by the data processor.

5

10

15

20

25

30

35

In one embodiment, once the application program knows the locale of a user, the number of the nearest network service provider located in the locale is dialed by the data processor via the modem. In other embodiments, the user may have a designated network service provider and the application program then dials the number of the designated network service provider and the appropriate country and area code. Optionally, the application program may provide the user with a choice as to whether they wish to use their designated network service provider or a network service provider in their present locale. Furthermore, the application program may provide the user with a choice of network service providers from which to choose in a particular location.

Typically, the network service provider is an Internet Service Provider (ISP) or an Internet Access Provider (IAP) which provides internet services to the user. Alternatively, the network service provider might be a proxy server of an intranet.

The network which the user uses to access the ISP does not have to be a telephone line but can be any sort of telecommunications network such as a telecommunications cable or telephony.

In some examples of the invention, the specific information contained on the data card includes the user's login identification and password which is required to access the ISP. The specific information may, however, contain other pieces of information, such as verification codes or encrypted

data relating to the user's finances or network preferences. This information can be used, for example, in the embodiment of the invention described in detail below wherein an online advertisement system accesses user profile information stored on a smart card to provide advertisements specifically tailored to the user's profile. This information may be inputted by the user upon initial use of the data card by having the user fill out a series of information fields. The personal information may then be encrypted and stored on the data card.

In some embodiments of the invention, the data processor is preferably a personal computer which includes or is connected to a modem which can access the internet. In other embodiments of the invention, the data processor may be housed within the data card reader, which may also include a graphical interface for the user to view information contained on the network.

According to another aspect of the present invention, there is disclosed a method for allowing a user to automatically access one of a plurality of network service providers which require information specific to the user and/or the network service provider to be accessed, comprising the steps of:

configuring an application program resident on a data processor to automatically retrieve at least part of the information specific to the user and/or the network service provider to be accessed contained on a data card when the data card is in communication with a data card reader and to use the information to gain access to one of the plurality of network service providers via a network by using one of a default access number indicating a designated network service provider and a local access number from a database containing a list of access numbers for the plurality of network service providers along with corresponding location information for each access number in the list; and

immediately triggering the application program upon insertion of the data card into the data card reader.

5 In another embodiment of the present invention, an online advertisement system provides advertisements to a user that are specifically tailored to the user's profile. The online advertisement system comprises:

a data card for storing information specific to the user, including user profile information;

10 a data card reader for accessing the information contained on the data card when the data card is in communication therewith;

a data processor in communication with the data card reader; and

15 an online advertising server connected to the data processor for serving the advertisements to the user, wherein the advertisements are specifically tailored to the user based on the user profile information.

20 In another embodiment of the present invention, a data card is provided for allowing a user to automatically access one of a plurality of network service providers, comprising:

25 a memory for storing information specific to the user and/or the plurality of network service providers and for storing an application program which is immediately triggered and which automatically uses the information to access one of the network service providers via a network when the data card is in communication with a data card reader that is communicating with a data processor.

In another embodiment of the present invention, a method is provided for automatically transferring information to a network, comprising the steps of storing the information on a data card, connecting to the network, and automatically uploading the information stored on the data card to the network upon connection thereto.

In another embodiment of the present invention, a system is provided for managing digital rights of digital content over a network, comprising: a data card which contains user information including digital rights information specific to a user, the data card having a memory component for enabling information to be stored within the data card; a data card reader adapted to access the user information contained on the data card when the data card is in communication therewith; a data processor in communication with the data card reader and adapted to be connected to the network; and an application program resident on the memory component of the data card, the application program being configured to operate in conjunction with a universal language for creating and controlling digital rights, to manage user rights of the digital content available on the network based on the digital rights information specific to the user which is contained on the data card.

The digital content may include at least one of e-books, e-magazines, e-newsletters, software, games, digital music, and digital video.

Upon initial use of the data card, the user may be prompted to initiate the data card by inputting personal identification information and authentication information into the data processor for encryption and storage on the data card. The personal identification information may include at least one of user name information, user address information, user gender information, user age information, and user government

identification information.

5 The digital rights information specific to the user may include access rights information and usage rights information. The application program may be further configured to automatically prompt the user to enter the authentication information for comparison with the authentication information stored on the data card, and to authorize the user following a match thereof to access and use the digital content in accordance with the access rights information and the usage rights information. 10 The usage rights information may include at least one of read-only rights, print rights, download rights, save rights, and distribution rights.

15 The application program may be further configured to track subsequent use of the digital content by the user. And the memory component of the data card may store an account balance of the user for payment of fees for accessing and using the digital content. The application program may be further configured to update the account balance of the user and to maintain profit information for an owner of the digital content. 20

25 In another embodiment of the present invention, a method is provided for managing digital rights of digital content over a network, comprising the steps of: storing user information on a data card having a memory component, including digital rights information specific to a user; and configuring an application program resident on the memory component of the data card to operate in conjunction with a universal language for creating and controlling digital rights for managing user rights of the digital content available on the network based on the digital rights information specific to the user which is contained on 30 the data card.

In another embodiment of the present invention, a data card is provided for allowing a user to access digital rights of digital content over a network, comprising: a memory for storing information including digital rights information specific to the user; a microprocessor for processing the information stored on the data card; a communications interface for transferring the information from the data card to a data card reader; and an application program resident on the memory and being configured to operate in conjunction with a universal language for creating and controlling digital rights, to manage user rights of the digital content available on the network based on the digital rights information specific to the user.

BRIEF DESCRIPTION OF DRAWINGS

Fig. 1 shows the logic for the smart card application trigger process;

Fig. 2 shows a trigger process wherein the application trigger polls a variable;

Fig. 3 shows an embodiment of the computer system in accordance with the present invention;

Fig. 4 shows an embodiment of the data card which is used in the data card reader of Fig. 3;

Fig. 5 shows in more detail the data card reader of Fig. 3;

Fig. 6 shows a number of stages which the system uses to connect a user automatically to the internet, in accordance with the present invention;

Fig. 7 shows a system including a remote server for serving specific advertisements to the user; and

Fig. 8 shows a system for managing digital rights of digital content over a network according to one embodiment.

BEST MODE FOR CARRYING OUT THE INVENTION

It is to be understood that the invention disclosed and defined herein extends to all alternative combinations of two or more of the individual features mentioned or evident from the text or drawings. All of these different combinations constitute various alternative aspects of the invention.

The foregoing describes embodiments of the invention, and modifications obvious to those skilled in the art can be made thereto without departing from the scope of the present invention.

Fig. 1 shows the logic for the smart card application trigger process. This diagram describes how a host application is launched upon insertion of the smart card. There are many different possible host applications. For example, the application trigger process could be used to access data sources through a network, launch local and remote applications for a particular user, boot a computing device, restrict access to computing platforms, allow entry into building facilities, or start a combustion or non-fossil engine.

As shown in Fig. 1, upon system and/or detection software power-up, boot, or reset as denoted by Start 86, the system moves to the trigger detection step 88 to wait for insertion of the smart card. Upon insertion of the card, data representing card insertion is sent to the trigger detector to be detected by the trigger detection step 88. Once the trigger is detected (i.e., the smart card is inserted), the application trigger 90 causes the host application to be launched.

Fig. 2 shows an alternative method for launching a host application upon insertion of the smart card. In Fig. 2, the trigger detection process is a continually running process that detects card insertion through smart card access attempts. The

application trigger 94 polls an O/S boolean variable that is set to either true or false upon trigger detection. Upon detecting the appropriate true/false value of the variable denoting insertion of the smart card, the application trigger 94 launches the application 96.

The launched application can be stored on the smart card itself, and the trigger detector and application trigger can be integrated into the same module. For example, upon trigger detection an application may be launched on the card by the application trigger logic to perform authentication processes on the smart card. Authentication is the verification of user identity through a personal identification number (PIN) stored on the host machine. For example, the application launched by the application trigger process may ask for a PIN from the user. To avoid this step, the user could store his or her PIN on the host machine. The trigger detector would then read data from a file with the stored PIN before starting the application trigger to verify the PIN. Alternatively, the PIN reading application could be launched as normal without prompting the user for a PIN but instead reading the PIN number from a file.

This process is distinguishable from the process used by magnetic strip reading automated teller machines (ATMs) since there is no embedded-chip present in such devices. ATMs are mechanical devices that perform a reading operation when a mechanical latch or switch movement is detected upon card insertion.

Next, the part of the system relating to automatic connection to a network according to the present invention will be described. Referring to Fig. 3, there is shown a computer system 10 which allows a user to automatically access a network service provider in the form of ISP 12. The ISP 12 requires the user's login identification and a password before the ISP 12

will provide access to the internet. This information is contained on a data card in the form of smart card 14 shown in Fig. 3 as being located within recess 16 that is within a data card reader in the form of smart card reader 18.

5 Upon first use of the smart card 14, the user may be required to input his or her personal information into the system using, for example, a series of information fields. This information is then encrypted and transferred onto the smart card 14.

10 The smart card reader 18 is adapted to read the login and password information for the ISP 12 that is contained on smart card 14. The smart card reader 18 is connected via cable 20 to a data processor in the form of central processing unit (CPU) 22 located within computer 24 (shown in this example of the invention by broken lines).

15 An application program 26 is resident in the memory of the computer 24, and contains code that allows the information contained on the smart card 14 to be processed by the CPU 22. The application program 26 is able to access information
20 contained in a database 28, which stores information relating to the ISP 12 as well as a number of other ISPs which are located in different locales. The database 28 may be stored on a CD ROM or on a remote server, for example. The application program 26 may be configured to either dial a default access
25 number previously stored on the smart card 14, or to read the area code from the smart card 14 and then dial a number from the database closely corresponding thereto. If there is no connection, a prompt asks the user to input the number to be dialed.

30 The computer 24 is also connected to a user graphical display in the form of monitor 32, which can display to the user information contained on the smart card 14 and information

which is downloaded from the ISP 12. The computer 24 also contains a modem 34 which establishes a link with ISP 12 via a network in the form of telephone line 30.

Referring now to Fig. 4, there is shown a cross-sectional view of the smart card 14. The smart card comprises a microprocessor 36 which can process information contained on the smart card 14, a memory component in the form of memory chip 38 which stores the information within the data card, a power source in the form of battery 40 which provides power to the microchip so that it can process information, and a communications interface in the form of contact connector 42. The contact connector 42 is exposed to the surface of one side of the smart card 14.

Referring now to Fig. 5, there is shown the smart card reader 18 with the recess 16 shown by broken lines. On one side of the smart card reader 18 there is provided an electrical connector 44 which is adapted to make contact with the contact connector 42 whenever the smart card 14 is inserted into recess 16.

Referring to Fig. 6, there is shown the steps for one typical method of the computer system according to the present invention, which will now be described in detail with reference also to Figs. 3, 4, and 5. When a user wishes to connect to the ISP 12 in order to access internet services such as the World Wide Web or internet mail service, the user inserts smart card 14 into recess 16 of the smart card reader 18. The electrical connector 44 detects that the smart card 14 is within the smart card reader 18 when the contact connector 42 makes physical contact with electrical connector 44. In this example of the invention, an activation code is generated by the microprocessor 36, which is then sent to the CPU 22 via cable 20. The CPU then relays this initiation code to the

application program 26. The first stage of this process can be seen as step 46 of Fig. 6.

Initially, the database is stored with the default telephone number of ISP 12 as a default so that the application program 26 automatically instructs the modem 34 to dial the telephone number of the ISP 12. The application program 26 then initiates a request code, requesting information relating to the login of the user for the ISP 12 from the smart card 14. The information from smart card 14 is then transferred from the memory chip 38 to the micro processor 36 out from the card via control connector 42 to electrical connector 44 and on to the CPU 22.

A routine call code is then generated to establish a link with ISP 12 as a call request as in step 48 of Fig. 6. The call request then activates modem 34 to place a call to ISP 12. If the telephone number of ISP 12 is correct, a connection is established with ISP 12 and the login information from smart card 14 can then be transmitted to the ISP 12.

The ISP 12 verifies that the login name and password are registered with the ISP in order to determine whether the call request is from an authorized user of the ISP 12. This can be seen at step 50 wherein the ISP 12 connection is made and the user is connected to the ISP 12 at step 52, or alternatively, if the identification is not verified as a registered user's login and password, the call request is terminated and the program exits (as can be seen at step 54).

In some circumstances, however, the user may be in another country and may not wish to use the ISP 12 but instead wishes to use another ISP which is not set as the default ISP in database 28. In such an instance, the local telephone number for ISP 12 would not work, as there is a different country code

and area code, or, alternatively, a different ISP telephone number.

5 In the situation where the user is in another country and wishes to use an ISP in the locale of the particular location in which he or she is in, the default connection to ISP 12 will not be established and the user will be at step 56 of Fig. 6. That is, the application program 26 will determine that the connection has not been established with ISP 12 and will
10 generate a list of countries from the database to the user on monitor 32.

15 The user then selects from the monitor 32 by using a mouse (not shown), the country in which they are in (e.g., the USA), as can be seen at step 58 of Fig. 6. The application program 26 then receives the selected country from the user and accesses the database 28 to retrieve all of the locales which are in the particular country. The locales are displayed to the user in the monitor 32 (as at step 60 of Fig. 6). The user then
20 selects the locale in which he or she is in at the particular time (i.e. such as Washington, D.C.).

25 The ISPs located within that particular locale are then displayed and the user selects a particular ISP from this list (as can be seen at stage 66 of Fig. 6). Another call request is then initiated as outlined above (this time for the new ISP) as can be seen by the loop 68 of Fig. 6. It is assumed that in such a situation, each ISP in a particular locale would have the same verification details of the smart card 14.

30 In another example of the invention, the smart card may not be used to select a new ISP, but may call the local ISP 12 (e.g., in Sydney, Australia when the user is in Washington, D.C.) by going through steps 46, 48, and then 56. Instead of the user
35 accessing an ISP in the particular locale he or she is

currently located in (as described above), the user could select a "direct connect" option which would request the user enter his or her current country location (e.g., USA) and locale (i.e., Washington, D.C.). The application will then determine the international dial-up connection number, the country number, and the area code of the country in which the ISP 12 is located (in this example, Sydney, Australia).

The information contained within the memory chip 38 may contain not only the user's login identification to the ISP 12, but may contain additional types of data, such as data to carry out a business transaction or data to automatically fill in particular information required on a form.

One example of such information which could automatically be updated on a form is information required by a bank for a personal loan. The smart card 14 could store data relating to the user's income, home address, whether the user's residence is owned or rented, the credit rating of the user and a summary of the spending habits relating to the user. The user would connect to the ISP 12 and connect to a web page of a bank. As the user connects to the bank's ISP 12, the user's information is automatically sent or uploaded to the bank via its ISP 12. The user would not have to fill out any forms via a keyboard, but could input upon interaction with the bank's web page how much he or she wished to loan from the bank. Alternatively, the bank could automatically calculate from the user's information which has been automatically uploaded to the bank the maximum amount of money that it is willing to loan the user. Such information could be displayed to the user from the bank's web page.

A particular advantage of the smart card 14 is that as the user's credit rating or spending habits change, the amount the bank is willing to lend him or her will also change.

Therefore, the user could quickly determine how much credit is available to him or her at any particular time, without having to fill out forms (either hardcopy forms or via a web page).

5 It should be further appreciated that the smart card 14 described herein does not have to be a contact smart card, but may in fact be a contactless smart card wherein the user accesses the ISP 12 whenever the smart card 14 (which in this example would have an antenna embedded within it) is passed
10 near the smart card reader 18.

15 In yet another example of the invention, the smart card reader and computer 24 may not be separate devices, but may in fact be combined into one piece of hardware so that the user can automatically access the ISP 12. Alternatively, it may be that the CPU 22, modem 34, and application program 26 are located within the smart card itself.

20 It should also be appreciated that the specific information contained on the data card may also relate to information other than the user's login and password for the ISP 12. The smart card may contain data specifying the network preferences of the user, such as the user's personal web page "book marks" and the specific Uniform Resource Locator (URL) of a particular web
25 site or personalized web page which is accessed whenever the user initially connects to the ISP 12. For example, the issuer of the smart card 14 may be a bank and the ISP 12 could be owned and managed by the bank. The user would be automatically connected to the bank's home page whenever smart card 14 is
30 inserted into smart card reader 18.

35 In another embodiment of the invention as shown in Fig. 7, the user is provided with online advertisement information that is specifically directed to the user's profile. The user's profile is determined from the personal identification

information stored on the smart card 80. The identification information may include the user's name, address, sex, social security number, credit card number, age, and income. Against this individual user information is allocated a profile code sequence that identifies for each information field a profile identifier. For example, corresponding to the user's income will be a code for identifying a range of income that the user falls within. And, corresponding to the user's zip code will be an identifying code for identifying the region the user comes from.

A remote online advertising server 82 for serving up banner advertisements to the user's personal computer 84 will read the profile codes from the smart card 80 using the smart card reader 86 and will then serve to the user's computer advertisements that are targeted according to the user's profile. In this way, the user is provided with advertisement information that is specifically directed to the user's profile.

Another embodiment of the invention relates to a system for digital rights management, using a smart card as the platform. The present disclosure provides a secure and individual identifying method of controlling access to and usage of various forms of digital data. These forms of digital data include the purchase and download of e-books and software, the pay per view of valuable and timely printed material such as industry newsletters, the pay per view of digital video, and the pay per listen or download of digital music. Combining digital rights management technology with a smart card-based payment and transaction system provides a tremendously useful application for digital-based transactions.

As described below, the present invention enables the information provider to control user access and use, and to

track subsequent use.

First, the present invention allows control of the user's access; that is, the user's right of entry to get to the digital information may be controlled. Control of access can be effected, for example, by way of passwords, encryption, and/or authentication.

The present invention also enables control over how the user can interface with the digital information. For example, the user may only be permitted read-only rights, thereby preventing the user from printing, saving, or distributing the digital information.

The present invention may also enable the information provider to track the subsequent use and/or distribution of its digital information online. This could be accomplished, for example, through the use of watermarking and digital footprints.

Furthermore, the present invention enables the information provider to generate revenue for the digital information accessed by the user.

The smart card designed in the manner as set forth by the present invention has, in addition to the above advantages, the capacity to store money transferred from a user's bank account to be used for micro payments over the internet and through wireless devices. This, coupled with digital rights management, provides the industry with a much needed system that to this point has not existed.

The present invention accomplishes its stated goals by, in one embodiment, combining the very high level security afforded by cryptographic smart cards with a universal language and standard for creating the terms and conditions associated with

digital rights management such as the well-known XrML (eXtensible rights Markup Language), which is licensed royalty-free. Combining smart card technology with such a language provides a universal method for specifying rights and issuing conditions associated with the use and protection of content. The present invention in one embodiment is a smart card-based platform for the interfacing with a language such as XrML in order to facilitate the creation of a very secure architecture for digital rights management. The present invention also uses cryptographic functions to store user information for use in online and off-line transactions with an electronic money purse function for real time micro-payments (e.g., small payments for a music clip). The universal language may be stored on the memory chip of the smart card, or provided via a server.

Fig. 8 shows a system for managing digital rights of digital content over a network according to one embodiment. A smart card or data card 92 includes a memory chip 95 for storing information including digital rights information specific to a user. The smart card 92 is located within a recess 94 that is within a smart card reader 96. The smart card reader 96 is adapted to access the information contained on the smart card 92 when the smart card 92 is in communication therewith.

A computer 100 has a central processing unit (CPU) 98, a random access memory (RAM) 102, and a hard disk 104. Removable storage capability is provided in 106, as well as a monitor 108 and input/output devices 110 such as a keyboard and mouse. The CPU 98 is connected to a modem 112, which provides access to a network 116.

An application program 114 resident on the memory chip 95 of the smart card 92 is configured to operate in conjunction with a universal language for creating and controlling digital rights, which may also be stored on the smart card 92, to

manage user rights of the digital content available on the network 116 based on the digital rights information specific to the user which is contained on the smart card 92. Alternatively, the application program 114 may be resident on the computer 100.

In this way, a system for managing digital rights of digital content over a network is taught by the present invention. The present invention is of major importance for technology players, owners of digital content, publishers, etc. Furthermore, the present invention may be rapidly integrated into various applications, including e-books and music. The rapid integration will come from the combined technological solution disclosed herein. The use of cryptographic smart cards are now being distributed in the millions. With the present invention, which in one embodiment is a combination cryptographic smart card with an interface controlling digital media rights such as XrML along with a secure instant payment system, is an optimal solution for both securing online data and for providing a secure instant transaction method for digitized products.

The present invention protects the rights of creators and publishers along with their content, collects their payment, and maintains their profits while providing consumers with easier access to content and lower prices.

The present invention provides an online trusted system for digital rights management. A trusted system using a standard language protects rights and enforce terms and conditions so that digital works can be authored and sold, then played or viewed on a wide variety of platforms. The rules interpreted by computers must be objective and consistent to enforce digital contracts. A trusted system refuses to perform an operation not licensed by a work's specific terms and conditions.

Terms and conditions governing the authorized use of a digital work may be expressed in a computer-interpretable language. And computers and software may be designed to enforce them. But a trusted system must resist physical tampering, detect misinformation from other digital systems, persistently reinforce terms and conditions, and resist unauthorized modifications.

Digital Rights Management facilitates the smooth, secure, trusted movement of digital works from creators and publishers to retailers and consumers. eContent owners assign rights and stipulate fees and access conditions governing the exercise of each specific right.

Digital rights management may allow aggregation, subscriptions, rentals and one-time transfers. There are unlimited combinations of embedded rights, terms and conditions controllable by digital rights management.

Use is simplified through computer-based rules providing consistent language and syntax. Compatibility is provided for all leading hardware and software platforms and the cost of implementation is reduced through off-the-shelf products utilized on commercial sites today. The present invention can be integrated with both existing systems and new ones as they are developed.

The above invention has been described with specific embodiments, but a person skilled in the art could introduce many variations on these embodiments without departing from the spirit of the disclosure or from the scope of the appended

claims. The embodiments are presented for the purpose of illustration only and should not be read as limiting the invention or its application. Therefore, the claims should be interpreted commensurate with the spirit and scope of the invention.

5

TOP SECRET